IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

KIMBERLY FARLEY, CHAD FORRESTER, and KIMBERLY SANDVIG, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	
v.	)	1:22-CV-468
EYE CARE LEADERS HOLDINGS, LLC,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Catherine C. Eagles, District Judge.

After receiving notice from their eye care clinics that their personal information had been implicated in a data breach, the plaintiffs Kimberly Farley, Chad Forrester, and Kimberly Sandvig began to worry about the future threat of identity theft. Mr. Forrester was soon the victim of a credit card fraud scheme, and Ms. Sandvig's credit score fluctuated dramatically despite no changes in her financial behavior. Believing these and other occurrences to be associated with the breach, the plaintiffs brought this class action lawsuit against the defendant, Eye Care Leaders Holdings, LLC (ECL), the entity that provides medical records platforms and patient management software to the plaintiffs' eye care clinics and whose data was breached.[1]

[1] The plaintiffs each originally brought separate lawsuits against ECL. The cases were consolidated for pre-trial purposes, *see* Docs. 23, 34, and together the plaintiffs filed an amended consolidated class action complaint, Doc. 31, which ECL now seeks to dismiss. Doc. 35.

ECL moves to dismiss this action for lack of subject-matter jurisdiction and failure to state a claim. Because the plaintiffs allege facts sufficient to plausibly establish standing and ECL's remaining arguments are better presented and evaluated on a more developed factual record, the motion will be denied.

I. Overview of Factual Allegations and Causes of Action

ECL provides record-keeping and healthcare software to eye care clinics across the country. Doc. 31 at ¶¶ 25–28. Through its services, ECL maintains and controls sensitive patient information. *Id.* at ¶¶ 29–31. Patients provide personal health information and identifying information to their clinics and physicians who store and manage that data through ECL. *Id.* This includes dates of birth, health insurance information, Social Security numbers, and health care information. *Id.* at ¶¶ 1, 30.

Ms. Farley, Mr. Forrester, and Ms. Sandvig provided their personal information to their eyecare clinics, each of which uses ECL's services. *Id.* at ¶¶ 17–19, 55–57, 62–64, 73–74. ECL controlled and managed access to the plaintiffs' information on behalf of the eyecare clinics. *Id.*

In 2021, ECL suffered from at least four data breaches, collectively referred to as "the data breach." *Id.* at ¶¶ 1, 3–7. In March 2021, "cybercriminals infiltrated ECL's computer systems and crippled a record-keeping system ECL provided to eye care clinics across the country." *Id.* at ¶ 3. During this breach, ECL "permanently lost control" over sensitive patient information. *Id.* at ¶¶ 38–39. A similar attack happened in April 2021, *id.* at ¶¶ 4, 41, and in August 2021 a former ECL employee "accessed ECL's systems and patient's Private Information." *Id.* at ¶ 6; *see also id.* at ¶ 42. In December 2021, another

breach "exposed substantial amounts of patients' Private Information." *Id.* at ¶ 43. The total number of data breach victims is approximately three million. *Id.* at ¶¶ 2, 45.

The plaintiffs' eyecare clinics notified them of the breach. *Id.* at ¶¶ 58–59, 65, 75. As a result of the data breach, each plaintiff has spent considerable time and effort monitoring accounts to protect or minimize harm from fraudulent activity. *Id.* at ¶¶ 61, 68, 82. Mr. Forrester was also "the victim of a credit card fraud scheme that resulted in an unauthorized and fraudulent charge" of about $150 on his credit card. *Id.* at ¶ 69. Ms. Sandvig's email has been hacked since the data breach, and someone changed her email address. *Id.* at ¶ 78. Her credit score "plummeted even though she had not changed any of her financial behavior for months," *id.* at ¶ 79, she "has been receiving a significantly higher number of spam emails and texts," and has "received a letter indicating that her" personal information "was recently found on the dark web," *id.* at ¶ 80, and she now "spends approximately $28 a month on data protection services." *Id.* at ¶ 81.

The plaintiffs bring claims for negligence, invasion of privacy, unjust enrichment, and breach of fiduciary duty. They assert federal jurisdiction under 28 U.S.C. § 1332(d), the Class Action Fairness Act.

II. Analysis

A. Standing

ECL contends that the plaintiffs' complaint should be dismissed because they fail to allege facts that plausibly show they have standing to sue. Doc. 36 at 7–17. This is a facial challenge to standing, so all well-pleaded facts in the complaint are accepted as

true and construed in the light most favorable to the plaintiffs. *See Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 208 (4th Cir. 2017).

"The doctrine of standing is an integral component of the case or controversy requirement" of federal jurisdiction. *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir. 2006). "The party invoking federal jurisdiction bears the burden of establishing" standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). The party "must demonstrate standing for each claim" and "for each form of relief" it seeks. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021).

Standing under Article III has three elements: (1) "the plaintiff must have suffered an injury in fact," (2) the injury must be "fairly traceable" to the defendant, and (3) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan*, 504 U.S. at 560–61 (cleaned up).

Injury in fact is the "invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (cleaned up). "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (cleaned up). "A concrete injury must be *de facto*; that is, it must actually exist." *Id.* at 340 (cleaned up). "[I]ntangible harms can also be concrete." *TransUnion*, 141 S. Ct. at 2204 (discussing how reputational harms, disclosure of private information, and abridgement of free speech qualify as concrete harms). Two recent Fourth Circuit cases provide helpful guidance in evaluating injury and traceability in a data breach case.

In *Beck v. McDonald*, the court considered two consolidated appeals brought by plaintiffs who sued a medical center after two data breaches compromised their personal information. 848 F.3d 262, 266–67 (4th Cir. 2017). In one underlying case, a laptop computer containing unencrypted patient information was either lost or stolen. *Id.* at 267. In the other, "four boxes of pathology reports headed for long-term storage" and containing personal information "had been misplaced or stolen." *Id.* at 268. In both cases, the plaintiffs alleged injury in fact based on an increased risk of identity theft, and the district court dismissed the claims for lack of standing. *Id.* at 267–69.

The Fourth Circuit affirmed, agreeing that the harms alleged were too speculative to establish standing because they required the court to engage with and credit an "attenuated chain of possibilities." *Id.* at 275 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410 (2013)). To find harm, the court would have to assume "that the thief targeted the stolen items for the personal information they contained" and that the thief would "then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities." *Beck*, 848 F.3d at 275. This chain of possibilities was not sufficient to confer standing, especially since there was no indication that the information had been stolen for the purpose of identity theft or that any plaintiff was the victim of identity theft. *Id.*

The next year, the Fourth Circuit considered *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc*, involving three optometrist-plaintiffs whose personal information was allegedly stolen when thieves stole data from the defendant, the National Board of Examiners in Optometry, Inc. 892 F.3d 613, 616 (4th Cir. 2018). Despite allegations

that after the data breach unauthorized persons opened credit cards in the plaintiffs' names, that their identities had thus been stolen, and that they had spent time and money on mitigation, the district court dismissed the claims for lack of standing. *Id.* at 617–18.

The Fourth Circuit distinguished the case from *Beck* and reversed, explaining that "[i]n *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes" containing personal information "had been stolen, but the information contained therein had not been misused." *Id.* at 621–22. In contrast, the plaintiffs in *Hutton* "allege[d] that they ha[d] already suffered actual harm in the form of identity theft and credit card fraud." *Id.* at 622. They had thus "been concretely injured by the data breach" because someone used or attempted to use their information to open credit cards without their knowledge. *Id.* Unlike in *Beck*, this harm was not speculative and was sufficient to allege injury in fact. *Id.*

The plaintiffs' cases are more like *Hutton* than *Beck*. Unlike in *Beck* where a laptop was either stolen or lost and four boxes of pathology reports were missing, *Beck*, 848 F.3d at 267–69, 274–75, thieves here targeted personal information in a series of massive and deliberate acts, giving rise to an easy inference that the thieves intended to misuse the personal information they stole. There may be many reasons unrelated to identity theft why someone might steal a laptop, such as obtaining the laptop itself, and it is not uncommon for old boxes of documents to be lost or misplaced. But one is hard pressed to think of a reason why data thieves would engage in a large-scale and sophisticated operation to steal electronic data containing personal information and only personal information other than to misuse it, either by identity theft or perhaps as part of

a blackmail or ransomware type scheme. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

As in *Hutton*, the plaintiffs have alleged that thieves targeted and stole personal information. *See, e.g.*, Doc. 31 at ¶¶ 1, 42, 93, 158. Unlike the plaintiffs in *Beck*, there are no other equally likely reasons for the theft. The Fourth Circuit in *Beck* implied that such allegations would be sufficient to establish standing, *see Beck*, 848 F.3d at 274, and other district courts have found such allegations of targeted data theft to be sufficient to establish standing. *See In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020) (finding standing when the defendant "disclosed that it was the target of" a cyberattack and distinguishing the case from *Beck* "where there were no allegations of targeting"); *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. 22-CV-747, 2022 WL 3919685, at *6 (D. Md. Aug. 31, 2022) ("[C]ourts have permitted a plaintiff to establish standing where the [personal identifying information] was the specific target of the attack.").

Like the plaintiffs in *Hutton*, Mr. Forrester and Ms. Sandvig also allege actual misuse of their information. At some point after the data beach, someone placed a fraudulent and unauthorized charge on Mr. Forrester's credit card. Doc. 31 at ¶ 69. Someone also hacked Ms. Sandvig's email, *id.* at ¶ 78, and her credit scored inexplicably plummeted and then fluctuated dramatically. *Id.* at ¶ 79. Additionally, Ms. Sandvig "has been receiving a significantly higher number of spam emails and texts." *Id.* at ¶ 80.

These injuries are sufficient to satisfy Article III standing.[2] *See Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 653 (4th Cir. 2019); *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921–22 (4th Cir. 2022); *McCreary v. Filters Fast LLC*, No. 20-CV-595, 2021 WL 3044228, at *4–5 (W.D.N.C. July 19, 2021).

Accepting the allegations in the complaint as true, the injuries are "fairly traceable" to ECL. *See Lujan*, 504 U.S. at 560. The "fairly traceable" standard is not the same as the tort causation standard. *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 161 (4th Cir. 2000). Instead, "[i]t must simply be *plausible* that" the data breach "was the cause" of the plaintiffs' injuries. *See Bank of La. v. Marriott Int'l, Inc.*, 438 F. Supp. 3d 433, 441 (D. Md. 2020). The plaintiffs have established standing to the extent required at this stage.

ECL also argues that the plaintiffs lack standing to seek prospective relief. Doc. 36 at 15–17. "A plaintiff can satisfy the injury-in-fact requirement for prospective relief either by demonstrating a sufficiently imminent injury in fact or by demonstrating an ongoing injury." *Garey*, 35 F.4th at 922 (cleaned up).

Accepting the allegations in the complaint as true, the plaintiffs have established a substantial risk of future injury. Some data breach victims have already experienced the

[2] Although Ms. Farley has not alleged actual misuse of her data, *see generally* Doc. 31, her allegations of targeted theft of personal information are sufficient to establish standing in the context of this case, especially since other plaintiffs have alleged actual misuse. *See In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 460 ("The allegations about the targeting of personal information in the cyberattack and the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent. In other words, in these circumstances the remaining . . . Plaintiffs do not have to wait until they, too, suffer identity theft to bring their claims to this court.").

misuse of their data, resulting in spam messages, hacked email addresses, fraudulent credit card charges, and adverse impacts to their credit scores. In these circumstances, the plaintiffs' fear of future injury is not just speculative. *See In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 460 ("The allegations about the targeting of personal information in the cyberattack and the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent."); *Desue v. 20/20 Eye Care Network, Inc.*, No. 21-CV-61275, 2022 WL 796367, at *5 (S.D. Fla. Mar. 15, 2022). They provide facts that plausibly allege a significant risk that ECL will again be targeted by data thieves, *see, e.g.*, Doc. 31 at ¶¶ 12, 16, 48, 119, and they allege that ECL continues to store their personal information. *Id.* at ¶ 119.

B. Failure to State a Claim

ECL argues that the laws of the plaintiffs' home states, Tennessee and Missouri, govern their claims and that under these laws all the claims fail. Doc. 36 at 18–24. In a diversity case, a federal district court applies the choice of law rules of the state in which it sits. *Perini/Tompkins Joint Venture v. Ace Am. Ins. Co.*, 738 F.3d 95, 100 (4th Cir. 2013). In tort and "tort-like" actions, North Carolina follows the rule of *lex loci*, applying the law of the state where the injury occurred. *SciGrip, Inc. v. Osae*, 373 N.C. 409, 420, 838 S.E.2d 334, 343 (2020); *Boudreau v. Baughman*, 322 N.C. 331, 335, 368 S.E.2d 849, 854 (1988) (applying law of the place where the injury occurred in a negligence case); *Harco Nat'l Ins. Co. v. Grant Thornton LLP*, 206 N.C. App. 687, 692, 698 S.E.2d 719, 722–23 (2010) (citing *Boudreau*, 368 S.E.2d at 853–54). This is ordinarily "the state

where the last event necessary to make the actor liable or the last event required to constitute the tort takes place." *SciGrip*, 838 S.E.2d at 343 (cleaned up).

Each cause of action must be evaluated separately to determine what the alleged injury is and where it allegedly occurred. *Boudreau*, 368 S.E.2d at 853–54 (analyzing causes of action separately for conflict of law purposes). This may be, but is not necessarily, the plaintiff's place of residence; the *lex loci* test "requires application of the law of the state where the plaintiff has actually suffered harm." *Harco*, 698 S.E.2d at 726 (applying the *lex loci* test to a misappropriation of trade secrets claim and rejecting the defendant's argument that the law where the plaintiff resided was automatically the law that applied).

In a data breach case applying the *lex loci* test under similar if not identical South Carolina law at the motion to dismiss stage, the United States District Court for the District of South Carolina has concluded that as to various negligence claims, the injury occurs when the data is stolen. *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 675 (D.S.C. 2021). The court applied the law of the state where the defendant was headquartered "because the place of the breach cannot be determined without further discovery and South Carolina is the only Blackbaud location specifically enumerated in the record." *Id.* at 676.

So too here. For purposes of the motion to dismiss, the Court will apply North Carolina law. *See, e.g.*, Doc. 31 at ¶¶ 20, 27 (providing that ECL is headquartered in Durham, North Carolina). A more definitive resolution of the choice of law question is deferred until "after the parties have developed the factual evidence through the process

of discovery," *Clean Earth of Md., Inc. v. Total Safety, Inc.*, No. 10-CV-119, 2011 WL 1627995, *4 (N.D.W. Va. Apr. 28, 2011), and with briefing that addresses more specifically where the injury ascribed to each cause of action arose. *See, e.g., In re Blackbaud, Inc.*, 567 F. Supp. 3d at 675 n.5 (collecting cases supporting this approach).

ECL argues that the plaintiffs fail to state any valid claim for relief under North Carolina law. But plaintiffs are not required to prove their case in the complaint. *See Robertson v. Sea Pines Real Est. Cos.*, 679 F.3d 278, 291 (4th Cir. 2012) ("*Iqbal* and *Twombly* do not require a plaintiff to prove his case in the complaint."). The plaintiffs have met the minimal standard of plausibility for each of their claims. Any weaknesses of those claims will be better evaluated on a more developed factual record.

III. Conclusion

The plaintiffs allege targeted data theft of their personal information as well as actual misuse of that information. These allegations are sufficient to support standing. And ECL's arguments on choice of law and otherwise are better evaluated on a more fully developed record. ECL's motion to dismiss will be denied. The defendant's motion to dismiss the plaintiff Jeanne Byers' complaint will be resolved in a separate order.

It is **ORDERED** that the defendant's motion to dismiss, Doc. 35, is **DENIED**.

This the 30th day of January, 2023.

UNITED STATES DISTRICT JUDGE